(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－251312
（P2001－251312A）
(43)公開日　平成13年９月14日(2001.9.14)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｑ　9/00	３０１Ｄ	５Ｋ０３３
Ｈ０４Ｑ　9/00	３０１		３２１Ｅ	５Ｋ０４８
	３２１	Ｈ０４Ｌ　11/00	３１０Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－59880(P2000－59880)

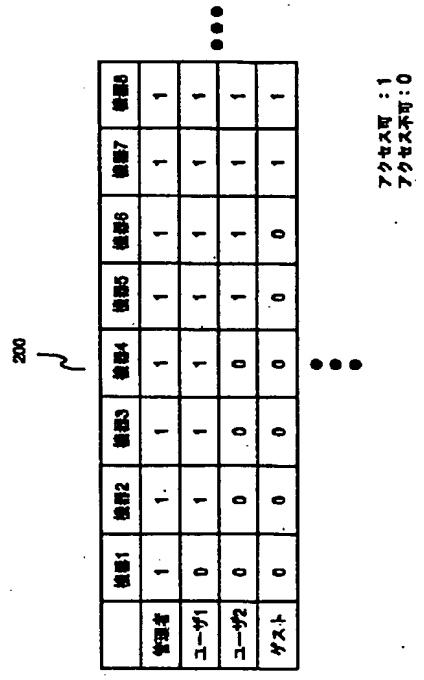
(22)出願日　平成12年３月６日(2000.3.6)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　井上　剛
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100102277
弁理士　佐々木　晴康　（外２名）

Ｆターム(参考)　5K033 AA08 BA01 CB01 DA01 DA06
DA17 DB12 DB16 DB18 EC04
5K048 AA15 BA12 BA13 CA08 DA02
DC04 DC07 EA11 EB02 EB03
FC01 GC05 HA01 HA02 HA05
HA07 HA21

(54)【発明の名称】　ホームネットワーク接続機器のアクセス管理装置

(57)【要約】
【課題】　機器毎、ユーザ毎、操作場所などによりアクセス管理を行ない、さらに、アクセスできる機器を変更することが可能なホームネットワーク接続機器のアクセス管理装置を提供する。
【解決手段】　ホームネットワーク１１１内に接続された機器に対する操作端末３００からのアクセス管理を行なうホームネットワーク接続機器のアクセス管理装置であって、前記ホームネットワーム１１１内のホームゲートウエイ１０１又はデータベース１０２などに、ユーザ毎に機器単位のアクセス許可情報を持つアクセス管理テーブル２００を設けている。



1

【特許請求の範囲】
【請求項１】　ホームネットワーク内に接続された機器に対する操作端末からのアクセス管理を行なうホームネットワーク接続機器のアクセス管理装置であって、
前記ホームネットワーム内に、ユーザ毎に機器単位のアクセス許可情報を持つアクセス管理テーブルを設けたことを特徴とするネットワーク接続機器のアクセス管理装置。
【請求項２】　前記請求項１に記載のネットワーク接続機器のアクセス管理装置において、
前記アクセス管理テーブルは、前記操作端末の場所に応じたアクセス許可情報を持つことを特徴とするネットワーク接続機器のアクセス管理装置。
【請求項３】　前記請求項１又は２に記載のネットワーク接続機器のアクセス管理装置において、
前記アクセス管理テーブルは、前記ホームネットワークにログインする際の第１のユーザ認証とは異なる第２のユーザ認証によりアクセスが許可され得るか否かを示すアクセス変更の許可情報を持つことを特徴とするネットワーク接続機器のアクセス管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ホームネットワーク内に接続された機器に対するアクセスを、ユーザや機器毎に管理することが可能なネットワーク接続機器のアクセス管理装置に関するものである。
【０００２】
【従来の技術】ホームネットワーク内に接続された家庭内の情報機器や家電機器を、ホームネットワークに接続された他の機器により操作する場合、ユーザ認証によってホームネットワークにログインが許可されると、該ホームネットワークに接続されている機器を全て操作することが可能である。
【０００３】図１３はホームネットワークに接続された機器を操作する時の処理を示すフローチャートである。まず、ホームネットワークにログインし（１４０１）、コマンド入力待ちとなる（１４０２）。
【０００４】操作端末から、ホームネットワークに接続された機器の操作コマンドを入力する（１４０３）と、当該機器にコマンドを発行する（１４０４）。このようにして、ホームネットワーク内に接続された機器を操作端末より操作することができる。
【０００５】
【発明が解決しようとする課題】しかしながら、上述した従来の技術においては、ホームネットワークへのログインが許可されると、ホームネットワークに接続された全ての機器を操作することが可能であり、家族以外の人や子供などに操作させたくない機器がネットワーク内に存在する場合に、その機器に対するアクセスを制限することができない。

2

【０００６】また、家族以外の人や子供がホームネットワーク内の機器を操作する場合、家族や大人がいる場合は操作できる機器を増やすというようなことができないという問題があった。
【０００７】さらに、例えば親の部屋にある機器を子供には操作させたくない場合や、その逆の場合など、アクセス制限を変更するのが望ましいが、ホームネットワーク内の機器を操作する時に、操作する場所によって、アクセス制限を変更することができないという問題があった。
【０００８】そしてまた、ホームネットワーク内から操作する時と、ホームネットワーク外（外出先など）から操作する時とで操作できる機器を制限する、或いは、家からの距離によって操作する機器を制限する、というようなことができないという問題があった。
【０００９】本発明は、上記課題に鑑みてなされたものであり、機器毎、ユーザ毎、操作場所などによりアクセス管理を行ない、さらに、アクセスできる機器を変更することが可能なホームネットワーク接続機器のアクセス管理装置を提供するものである。
【００１０】
【課題を解決するための手段】本願の第１の発明は、ホームネットワーク内に接続された機器に対する操作端末からのアクセス管理を行なうホームネットワーク接続機器のアクセス管理装置であって、前記ホームネットワーム内に、ユーザ毎に機器単位のアクセス許可情報を持つアクセス管理テーブルを設けたことを特徴とするものである。
【００１１】これによって、例えば家族以外の人（ゲスト）や子供などに操作させたくない機器がホームネットワーク内に存在する時にも、ユーザ毎に設定された機器単位のアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。
【００１２】本願の第２の発明は、前記アクセス管理テーブルは、前記操作端末の場所に応じたアクセス許可情報を持つことを特徴とするものである。ここで、操作端末の場所とは、ホームネットワークからの距離、ホームネットワークが構築されている屋内の部屋、ホームネットワークの内外などによって規定される。
【００１３】これによって、例えば操作する場所によって操作させたくない機器がホームネットワーク内に存在する場合にも、操作を行なう場所に応じたアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。
【００１４】また、操作する場所がホームネットワーク内か、ホームネットワーク外かによって操作させたくない機器がホームネットワーク内に存在する場合にも、操作させたくない機器に対するアクセスを制限することができる。
【００１５】本願の第３の発明は、前記アクセス管理テ

ーブルは、前記ホームネットワークにログインする際の第１のユーザ認証とは異なる第２のユーザ認証によりアクセスが許可され得るか否かを示すアクセス変更の許可情報を持つことを特徴とするものである。

【００１６】これによって、例えば家族以外の人（ゲスト）や子供がホームネットワーク内の機器を操作する時に、第２のユーザ認証を行ない、認証されたユーザのアクセス許可情報に基づいて、家族や大人がいる場合は操作できる機器を増やすというようなことを実現することができる。

【００１７】

【発明の実施の形態】以下、本発明の第１実施形態について、図１乃至図４とともに詳細に説明する。

【００１８】図１は本実施形態におけるシステム構成例を示す説明図である。図1において、１０１はホームネットワーク１１１に接続される機器の管理や公衆ネットワーク１１２とホームネットワーク１１１との接続などをするホームゲートウェイ（以下、ＨＧＷ）、１０２は各種情報を保管するデータベースである。

【００１９】１０３、１０４、１０５、１０６はホームネットワーク１１１に接続された端末Ａ、端末Ｂ、端末Ｃ、端末Ｄ、１０８、１０９、１１０は同じくホームネットワーク１１１に接続された無線端末Ａ、無線端末Ｂ、無線端末Ｃ、１０７は無線端末Ａ１０８、Ｂ１０９、Ｃ１１０を管理するアクセスポイント（ＡＰ）である。

【００２０】尚、上記端末Ａ１０３、Ｂ１０４、Ｃ１０５、Ｄ１０６および無線端末Ａ１０８、Ｂ１０９、Ｃ１１０は、ＡＶ機器や、エアコン、湯沸し器等の家屋内にある電機製品や、パソコン等の情報機器、電話等の通信機器、それを操作するためのリモコン、ＰＤＡ等である。

【００２１】図２は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル２００は、図２に示すように、ホームネットワーク１１１に接続されるユーザ毎に機器単位のアクセス許可／不許可の情報を持つテーブルであり、ホームネットワーク１１１内のデータベース１０２、または、ＨＧＷ１０１内などに保管されている。

【００２２】前記アクセス管理テーブル２００は、ホームネットワーク１１１に新たな機器を接続する場合に、ユーザ毎にその機器のアクセス許可／不許可情報が追加される。また、新しいユーザを登録する場合に、各機器に対して新しいユーザのアクセス許可／不許可情報が追加される。

【００２３】図３はホームネットワーク１１１内に接続された機器を操作するための操作端末の一例を示すブロック図である。この操作端末３００は、図３に示すように、ユーザに対して情報を提示する表示部３０１と、文字、画像、音声情報などを入力する入力部３０２と、ネットワークと接続するネットワークインタフェイス部３０３と、メモリ部３０４と、上記各部３０１～３０４をコントロールする処理部３０５とを有している。

【００２４】図４は操作端末３００からホームネットワーク１１１内の機器を操作する時の処理を示すフローチャートである。以下、図４を参照してユーザ毎に機器単位のアクセス管理を行なう方法を詳しく説明する。

【００２５】まず、操作端末３００の入力部３０２から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう（４０１）。ここでは、操作端末３００内のメモリ部３０４に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部３０３を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して認証を行なう。

【００２６】ユーザが認証されると、ホームネットワーク１１１内のデータベース１０２またはＨＧＷ１０１のアクセス管理テーブル２００から、ログインしたユーザのアクセス制御テーブルを、ネットワークインターフェイス部３０３を介して取得し（４０２）、メモリ部３０４に保存した後、操作コマンドの入力待ちになる（４０３）。

【００２７】次に、入力部３０２から、ホームネットワーク１１１内の機器を操作する制御コマンドが入力される（４０４）と、メモリ部３０４内のアクセス制御テーブルとの照合を行なう（４０５）。

【００２８】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部３０３を介して送信する（４０６）。アクセス不可能であれば、当該機器の制御が不可能であることをユーザに対して表示部３０１より通知し（４０７）、操作コマンドの入力待ちに戻る（４０３）。

【００２９】以上のように、本実施形態においては、ホームネットワーク１１１内に、ユーザ毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル２００を設けているので、ユーザ毎にホームネットワーク１１１に接続された機器単位のアクセス管理を行なうことができる。

【００３０】次に、本発明の第２実施形態について、図５及び図６とともに説明するが、上記第１実施形態と同一部分には同一符号を付し、その説明は省略する。

【００３１】本実施形態においては、ホームネットワーク１１１に接続されたアクセス管理装置を設けている。尚、このアクセス管理装置は、ホームネットワーク１１１を管理するＨＧＷ１０１に直接接続しても、ＨＧＷ１０１に内蔵しても良い。

【００３２】図５は本実施形態のアクセス管理装置を示すブロック図である。このアクセス管理装置６００は、図５に示すように、ユーザ毎に機器単位のアクセス許可／不許可を示すテーブル情報や、ユーザの認証に必要な情報を保管するメモリ部６０１と、ネットワークと接続

5

するネットワークインタフェイス部６０２と、上記各部６０１、６０２をコントロールする処理部６０３とを有している。

【００３３】メモリ部６０１には、図２とともに上述した第１実施形態におけるアクセス管理テーブル２００が保管される。上記第１実施形態と同様、ホームネットワーク１１１に新たな機器を接続する場合、ユーザ毎にその機器のアクセス許可／不許可情報をアクセス管理テーブル２００に追加し、新しいユーザを登録する場合、各機器に対して新しいユーザのアクセス許可／不許可情報をアクセス管理テーブル２００に追加する。

【００３４】ホームネットワーク１１１に接続された機器は、図３とともに上述した第１実施形態における操作端末３００を使用して操作される。図６は操作端末３００からホームネットワーク１１１内の機器を操作する時の処理を示すフローチャートである。以下、図６を参照してユーザ毎に機器単位のアクセス管理を行なう方法を詳しく説明する。

【００３５】まず、操作端末３００の入力部３０２からユーザ名、パスワード等を入力し、ユーザのログインを行なう（７０１）。ここでは、操作端末３００内のメモリ部３０４に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部３０３を介して、ＨＧＷ１０１またはアクセス管理装置６００内のメモリ部６０１の情報に基づき、ユーザ名、パスワード等を送信して認証を行なう。

【００３６】ユーザが認証されると、操作コマンド入力待ちとなり（７０２）、入力部３０２から、ホームネットワーク１１１内の機器を操作する制御コマンドが入力される（７０３）と、ネットワークインターフェイス部３０３を介して、アクセス管理装置６００にユーザ情報と操作機器情報を送信し、制御の可否を確認する（７０４）。

【００３７】この時、アクセス管理装置６００では、メモリ部６０１に保存されているアクセス管理テーブル２００の情報と受信したユーザ情報、操作機器情報とからアクセスの可否を判断し、判断結果を操作端末３００へ送信する。

【００３８】次に、アクセスが可能であれば、機器制御コマンドを制御対象の機器に対して送信し（７０５）、アクセス不可能であれば制御が不可能であることをユーザに対して表示部３０１より通知し（７０６）、操作コマンド入力待ち（７０２）に戻る。

【００３９】以上のように、本実施形態においては、ホームネットワーク１１１内に、ユーザ毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル２００を有するアクセス管理装置６００を設けているので、ユーザ毎にホームネットワーク１１１に接続された機器毎のアクセス管理を行なうことができる。

【００４０】尚、上述した第１実施形態においては、ログイン時にＨＧＷなどからアクセス管理テーブルの情報を取得するが、この場合ホームネットワークに接続されるどの機器に対してもアクセスする可能性があるので、すべての機器の情報を取得する必要があり、ログイン時に大量のデータが通信される。

6

【００４１】これに対して、本実施形態においては、操作コマンド毎にアクセス管理装置に問い合わせる場合は、操作コマンドとユーザ情報とそれに対する許可／不許可の情報とが通信されるだけなので、通信データ量を低減させることが可能である。

【００４２】また、上記第１実施形態では、アクセス管理テーブルとユーザ認証情報とが、別の機器に記録されている場合があるが、その場合、操作端末からコマンドを発行する時と認証の時とでそれぞれ別の機器に問い合わせなければならない。そこで、本実施形態においては、アクセス管理テーブルやユーザ認証情報などを一つの機器に記録しているので、操作端末から問い合わせる際に１つの機器で済む。

【００４３】次に、本発明の第３実施形態について、図７及び図８とともに説明するが、上記第１実施形態と同一部分には同一符号を付し、その説明は省略する。

【００４４】本実施形態においては、ホームネットワークに接続された機器を操作する機器の場所によってアクセス管理を行なうものであり、主にホームネットワーク外（屋外）からの操作に対するアクセス管理を行なうものである。

【００４５】図７は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル８００は、図７に示すように、上記第１実施形態におけるアクセス管理テーブル２００に、操作を行なう場所の情報を追加したものである。

【００４６】ここで、操作を行なう場所の情報とは、例えば家と操作端末との距離であり、事前に各ユーザ、各機器毎に操作端末との距離に応じたアクセスの可または不可を決定し、アクセス管理テーブル８００に登録しておく。

【００４７】図８はホームネットワーク内に接続された機器を操作するための操作端末の一例を示すブロック図である。この操作端末９００は、図８に示すように、ユーザに対して情報を提示する表示部９０１と、文字、画像、音声情報などを入力する入力部９０２と、ネットワークと接続するネットワークインタフェイス部９０３と、メモリ部９０４とを有している。

【００４８】さらに、ＧＰＳまたは公衆ネットワークの基地局等から送信される位置情報などに基づき、操作端末の位置情報を取得して保存する位置情報取得部９０５と、上記各部９０１～９０５をコントロールする処理部９０６とを有している。

【００４９】上記位置情報取得部９０５は、一定の時間毎に位置情報を取得して更新するか、入力部９０２によ

り入力された命令によって位置情報を取得し更新する。

【００５０】以下、操作端末９００からホームネットワーク１１１内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【００５１】まず、操作端末９００の入力部９０２から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、操作端末９００内のメモリ部９０４に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部９０９を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して認証を行なう。

【００５２】ユーザが認証されると、アクセス管理テーブル２００を持つデータベース１０２またはＨＧＷ１０１などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部９０３を介して取得し、メモリ部９０４に保存した後、操作コマンド入力待ちになる。

【００５３】次に、入力部９０２から、ホームネットワーク１１１内の機器を操作する制御コマンドが入力されると、ログイン時のユーザ情報と入力されたコマンドとから得られる操作する機器の情報、位置情報取得部９０５の位置情報を、メモリ部９０４内のアクセス制御テーブルと照合する。

【００５４】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部９０３を介して送信し、アクセス不可能であれば、当該機器の制御が不可能であることをユーザに対して表示部９０１より通知し、操作コマンド入力待ちに戻る。

【００５５】尚、ログイン時にＨＧＷ１０１などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図６とともに上述した第２実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

【００５６】以上のように、本実施形態においては、ホームネットワーク１１１内に、各ユーザの場所（距離）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル８００を設けているので、ホームネットワーク１１１に接続された機器を操作する操作端末９００の場所（距離）によって、アクセス管理を行なうことができる。

【００５７】次に、本発明の第４実施形態について、図９とともに説明するが、上記第３実施形態と同一部分には同一符号を付し、その説明は省略する。

【００５８】本実施形態においては、ホームネットワーク１１１に接続された機器を操作する機器の場所によってアクセス管理を行うものであり、主にホームネットワーク内（屋内）からの操作に対するアクセス管理を行うものである。

【００５９】図９は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル１０００は、図９に示すように、上記第１実施形態におけるアクセス管理テーブル２００に、操作機器により操作を行なう場所の情報を追加したものである。

【００６０】上記場所の情報とは、例えば操作する機器に対するアクセスを許す部屋のリストであり、事前に各ユーザ、各機器毎に操作端末のある部屋に応じたアクセスの可または不可を決定し、アクセス管理テーブル１０００に登録しておく。

【００６１】以下、操作端末９００からホームネットワーク１１１内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【００６２】まず、操作端末９００の入力部９０２から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、操作端末９００内のメモリ部９０４に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部９０９を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して認証を行なう。

【００６３】ユーザが認証されるとアクセス管理テーブル１０００を持つデータベース１０２またはＨＧＷ１０１などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部９０３を介して取得して、メモリ部９０４に保存した後、操作コマンド入力待ちになる。

【００６４】次に、入力部９０２から、ホームネットワーク１１１内の機器を操作する制御コマンドが入力されると、位置情報取得部９０５の位置情報とメモリ部９０４内のアクセス制御テーブル１０００とを照合する。

【００６５】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部９０３を介して送信し、アクセス不可能であれば、制御が不可能であることをユーザに対して表示部９０１より通知し、操作コマンド入力待ちに戻る。

【００６６】尚、ログイン時にＨＧＷ１０１などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図６とともに上述した第２実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

【００６７】以上のように、本実施形態においては、ホームネットワーク１１１内に、各ユーザの場所（部屋）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル１０００を設けているので、ホームネットワーク１１１に接続された機器を操作する操作端末９００の場所（部屋）によって、アクセス管理を行なうことができる。

【００６８】次に、本発明の第５実施形態について、図１０とともに説明するが、上記第１実施形態と同一部分には同一符号を付し、その説明は省略する。

【００６９】上述した第３実施形態および第４実施形態

をどちらも実施し、ホームネットワーク外（屋外）およびホームネットワーク内（屋内）の場所によって、アクセス管理を行なうことができるが、この場合、屋外の場合は距離毎に、屋内の場合は部屋毎に、アクセスの可否を決定し設定しておかなければならず、また、アクセス管理テーブルが大きくなる。

【００７０】そこで、本実施形態においては、設定を簡略化するために、ホームネットワーク外からのアクセスと、ホームネットワーク内からのアクセスとの２通りのアクセスの可否を表すアクセス管理テーブルを備える。

【００７１】図１０は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル１１００は、図１０に示すように、ホームネットワーク１１１外（屋外）、およびホームネットワーク１１１内（屋内）からのアクセス許可／不許可の情報を持つテーブルである。

【００７２】以下、操作端末３００からホームネットワーク１１１内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【００７３】まず、操作端末３００の入力部３０２から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、ネットワークインターフェイス部３０３を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して認証を行なう。

【００７４】この時、ＨＧＷ１０１はホームネットワーク１１１外からのアクセスかホームネットワーク内からのアクセスかを判断できるので、その判断結果を操作端末３００に送信し、操作端末３００はその情報をメモリ部３０４に記録する。

【００７５】ユーザが認証されると、アクセス管理テーブル１１００を持つデータベース１０２またはＨＧＷ１０１などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部３０３を介して取得して、メモリ部３０４に保存、操作コマンド入力待ちになる。

【００７６】次に、入力部３０２から、ホームネットワーク１１１内の機器を操作するコマンドが入力されると、ログイン時のユーザ情報と入力されたコマンドから得られる操作する機器の情報と、メモリ部３０４内の位置情報と、アクセス制御テーブルとを照合する。

【００７７】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部３０３を介して送信し、アクセス不可能であれば、制御が不可能であることをユーザに対して表示部３０１より通知して、操作コマンド入力待ちに戻る。

【００７８】尚、ログイン時にＨＧＷ１０１などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図６とともに上述した第２実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

【００７９】以上のように、本実施形態においては、ホームネットワーク１１１内に、各ユーザの場所（屋内外）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル１１００を設けているので、ホームネットワーク１１１に接続される機器を操作する操作端末３００の場所（屋内外）によって、アクセス管理を行なうことができる。

【００８０】次に、本発明の第６実施形態について、図１１及び図１２とともに説明するが、上記第１実施形態と同一部分には同一符号を付し、その説明は省略する。

【００８１】本実施形態においては、ホームネットワーク１１１に接続された機器のアクセスの管理をユーザによって管理する時、第２のユーザ認識をすることによって、アクセスできるホームネットワーク内の機器を変更することができるものである。

【００８２】図１１は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル１２００は、図１１に示すように、上記第１実施形態におけるアクセス管理テーブル２００に、アクセス権限の変更の可否を表す情報を追加したものである。

【００８３】前記アクセス管理テーブル１２００は、ホームネットワーク１１１に新たな機器を接続する場合に、ユーザ毎にその機器のアクセス許可／不許可情報が追加される。また、新しいユーザを登録する場合に、各機器に対して新しいユーザのアクセス許可／不許可情報が追加される。

【００８４】以下、操作端末３００からホームネットワーク１１１内の機器を操作する時の処理（アクセス管理）について、特に第２のユーザ認識によりアクセスできるホームネットワーク１１１内の機器を変更する方法を、図１２を用いて詳しく説明する。

【００８５】まず、操作端末３００の入力部３０２から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、ネットワークインターフェイス部３０３を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して第１のユーザ認証を行なう。

【００８６】第１のユーザ認証がなされると、アクセス管理テーブル１２００を持つデータベース１０２またはＨＧＷ１０１などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部３０３を介して取得して、メモリ部３０４に保存した後、操作コマンド入力待ちになる。

【００８７】次に、入力部３０２から、ホームネットワーク１１１内の機器を操作する制御コマンドを入力すると、メモリ部３０４内のアクセス制御テーブルとの照合を行ない、制御の可否を確認する。

【００８８】ここで、ホームネットワーク１１１内の機器を操作できなかった時、アクセス管理テーブル１２００を参照して、アクセス権限が変更可能であるか否かを判断する（１３０１）。

11

【００８９】このとき、アクセス権限の変更が不可である場合は、制御が不可能であることをユーザに対して表示部３０１より通知し、操作コマンド入力待ちに戻る。

【００９０】アクセス権限が変更可能である場合は、ユーザに対して第２のユーザ認証を行なうことにより操作できることを、表示部３０１より通知して（１３０２）、パスワードの入力要求を行なう（１３０３）。

【００９１】ユーザは、第２のユーザ認証に必要なユーザ名、パスワード（ネットワークにログインする際の第１のユーザ認証に必要なパスワードとは異なるパスワード）等を入力する（１３０４）。

【００９２】そして、操作端末３００内のメモリ部３０４に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部３０３を介して、ＨＧＷ１０１にユーザ名、パスワード等を送信して第２のユーザ認証を行なう。

【００９３】第２のユーザ認証がなされると、機器に対して制御コマンドをネットワークインターフェイス部３０３を介して送信し、第２のユーザ認証がなされなかった時は、制御が不可能であることをユーザに対して表示部３０１より通知し、操作コマンド入力待ちに戻る。

【００９４】以上のように、本実施形態においては、ホームネットワーク１１１内に、各ユーザ毎に機器単位のアクセス権限の変更の可否を表す情報を持つアクセス管理テーブル１２００を設けているので、第２のユーザ認識を行なうことによって、アクセスできるホームネットワーク１１１内の機器を変更することができる。

【００９５】例えば、ある機器に対して、子供だけでいるときには、アクセス（操作）させたくないが、親がそばにいるときには、アクセス（操作）を許したいというような場合、第２のユーザ認証を行なうことにより、ホームネットワーク１１１にログインしたときの状態に比べて、アクセス（操作）できる機器を増やすことができる。

【００９６】尚、本発明を実施するにあたっては、上述した各実施形態を組み合わせても良いことは明らかである。例えば、操作端末の場所に応じて、アクセス権限の変更可否を切り替えるなど、適宜実施することが可能である。

【００９７】

【発明の効果】本願請求項１の発明によれば、例えば家族以外の人（ゲスト）や子供などに操作させたくない機器がホームネットワーク内に存在する時にも、ユーザ毎に設定された機器単位のアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。

【００９８】本願請求項２の発明によれば、例えば操作する場所によって操作させたくない機器がホームネットワーク内に存在する場合にも、操作を行なう場所に応じたアクセス許可情報に基づいて、操作させたくない機器

12

に対するアクセスを制限することができる。

【００９９】また、操作する場所がホームネットワーク内か、ホームネットワーク外かによって操作させたくない機器がホームネットワーク内に存在する場合にも、操作させたくない機器に対するアクセスを制限することができる。

【０１００】本願請求項３の発明によれば、例えば家族以外の人（ゲスト）や子供がホームネットワーク内の機器を操作する時に、第２のユーザ認証を行ない、認証されたユーザのアクセス許可情報に基づいて、家族や大人がいる場合は操作できる機器を増やすというようなことを実現することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態におけるシステム構成を示す説明図である。

【図２】本発明の第１実施形態におけるアクセス管理テーブルを示す説明図である。

【図３】本発明の第１実施形態における操作端末の概略構成例を示すブロック図である。

【図４】本発明の第１実施形態における操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【図５】本発明の第２実施形態におけるアクセス管理装置を示す説明図である。

【図６】本発明の第２実施形態における操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【図７】本発明の第３実施形態におけるアクセス管理テーブルを示す説明図である。

【図８】本発明の第３実施形態における操作端末の概略構成例を示すブロック図である。

【図９】本発明の第４実施形態におけるアクセス管理テーブルを示す説明図である。

【図１０】本発明の第５実施形態におけるアクセス管理テーブルを示す説明図である。

【図１１】本発明の第６実施形態におけるアクセス管理テーブルを示す説明図である。

【図１２】本発明の第６実施形態における操作端末からホームネットワーク内の機器を操作する時の処理の要部を示すフローチャートである。

【図１３】従来の操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【符号の説明】

１０１　ホームゲートウェイ
１０２　データベース、
１０３～１０６　接続機器
１０７～１１０　無線端末
１１１　ホームネットワーク、
１１２　公衆ネットワーク
２００、８００、１０００、１２００　アクセス管理テ

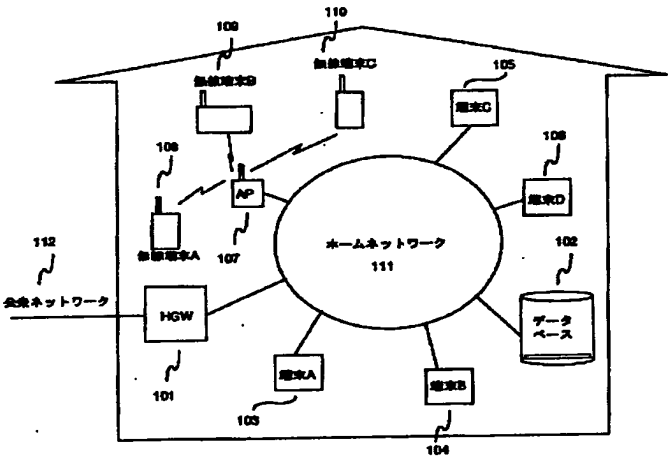
13

ーブル
３００、９００　操作端末
３０１、９０１　表示部
３０２、９０２　入力部
３０３、９０３　ネットワークインターフェイス部
３０４、９０４　メモリ部

14

＊３０５、９０６　処理部
９０５　位置情報取得部
６００　アクセス管理装置
６０１　メモリ部
６０２　ネットワークインターフェイス部
＊　６０３　処理部

【図１】



【図２】

200

	機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
管理者	1	1	1	1	1	1	1	1
ユーザ1	0	1	1	1	1	1	1	1
ユーザ2	0	0	0	0	1	1	1	1
ゲスト	0	0	0	0	0	0	1	1

アクセス可　：1
アクセス不可：0

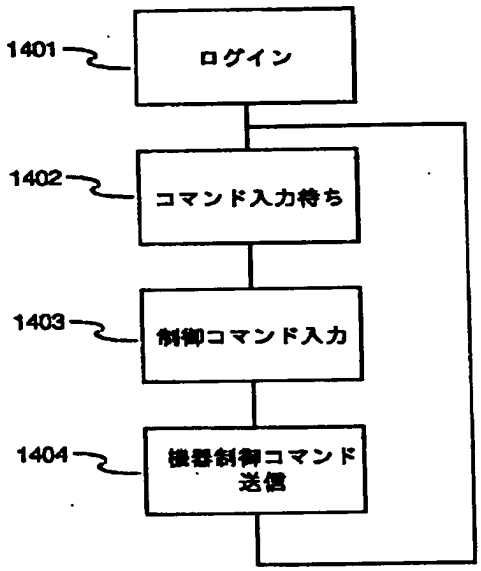
【図１１】

1200

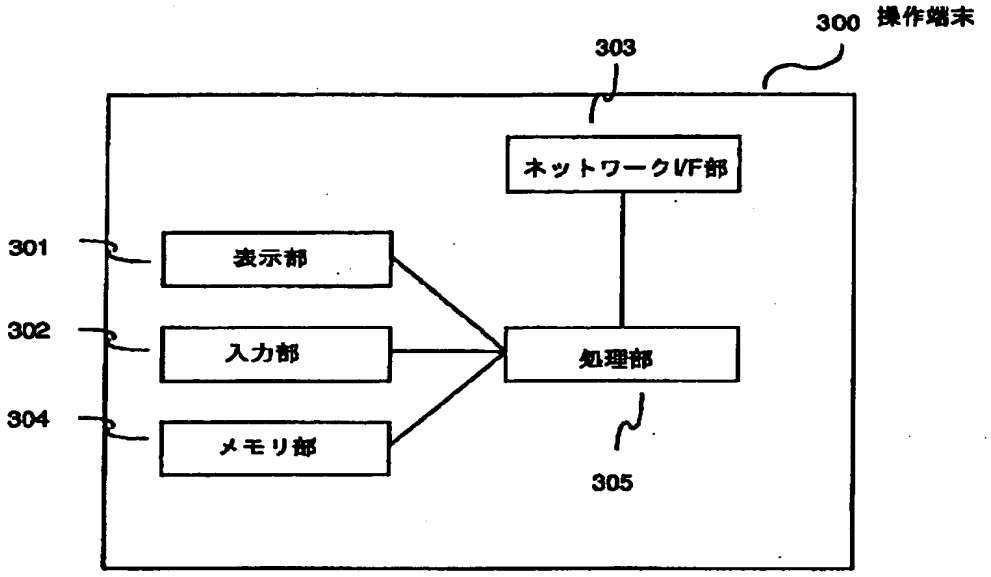
	機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
管理者	2	2	2	1	1	1	1	1
ユーザ1	2	1	1	1	1	1	1	1
ユーザ2	0	0	2	2	1	1	1	1
ゲスト	0	0	0	0	2	2	1	1

アクセス可　　：2
アクセス変更可：1
アクセス不可　：0

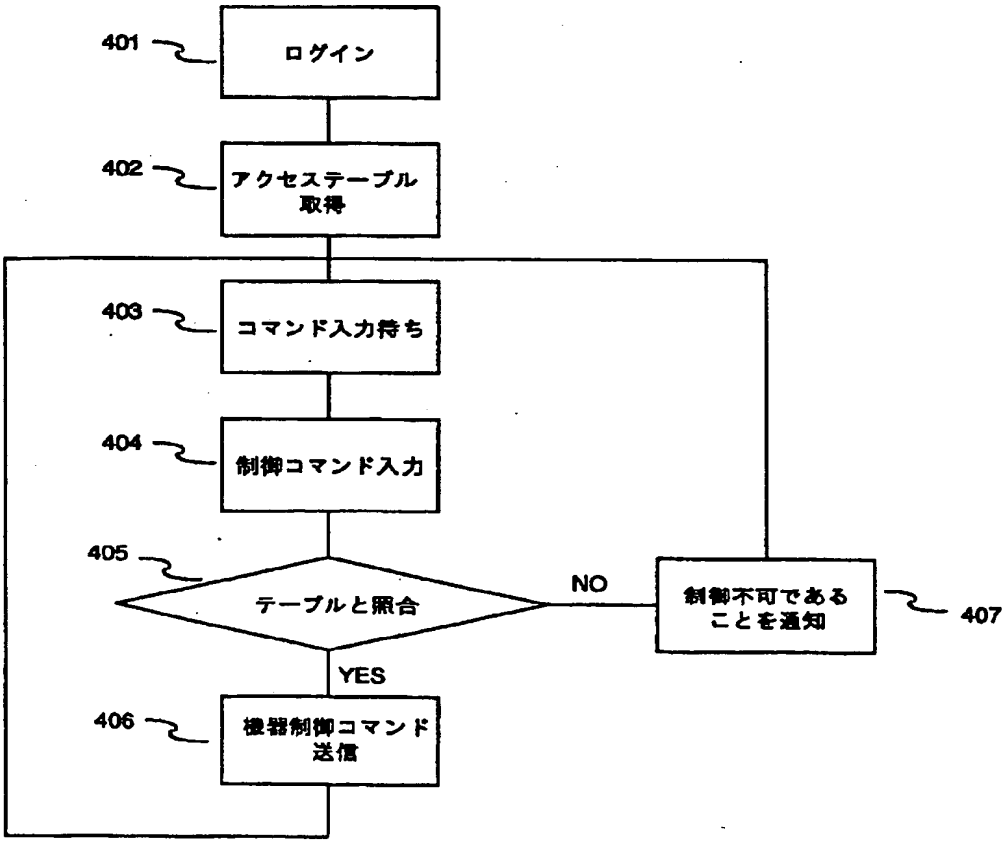
【図１３】



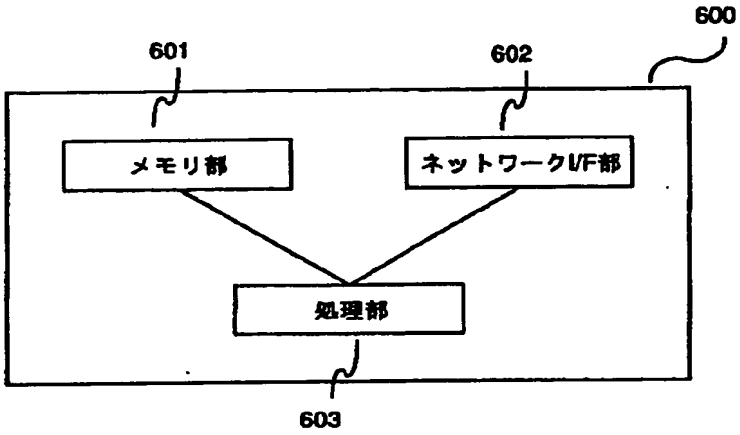
【図３】


300 操作端末
303
ネットワークI/F部
301
表示部
302
入力部
304
メモリ部
処理部
305

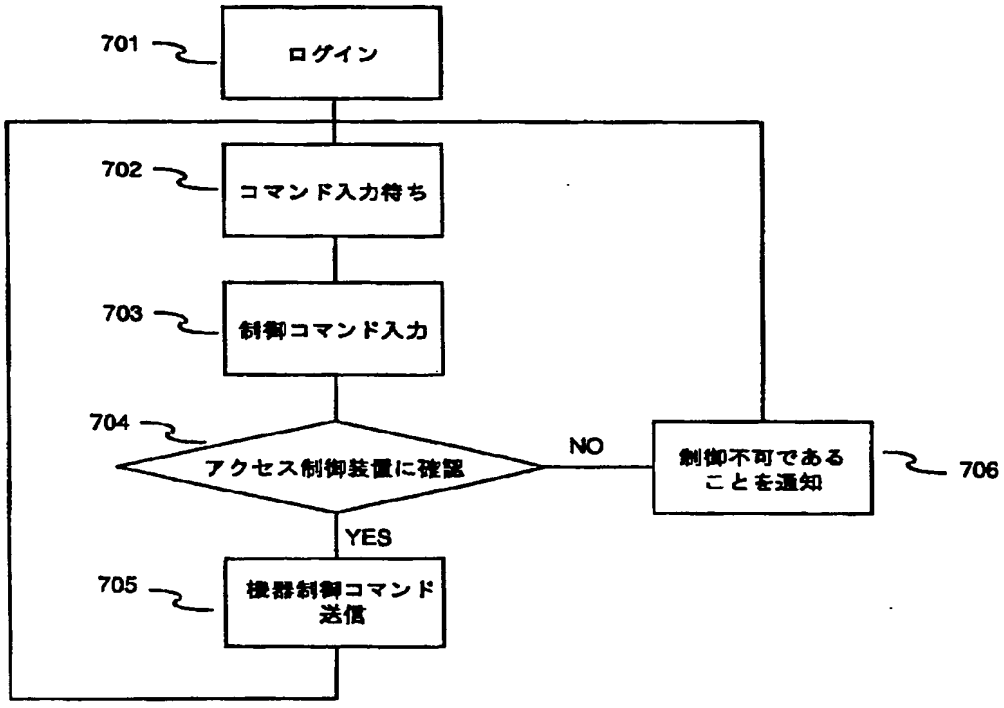
【図４】


401
ログイン
402
アクセステーブル取得
403
コマンド入力待ち
404
制御コマンド入力
405
テーブルと照合
NO
制御不可であることを通知
407
YES
406
機器制御コマンド送信

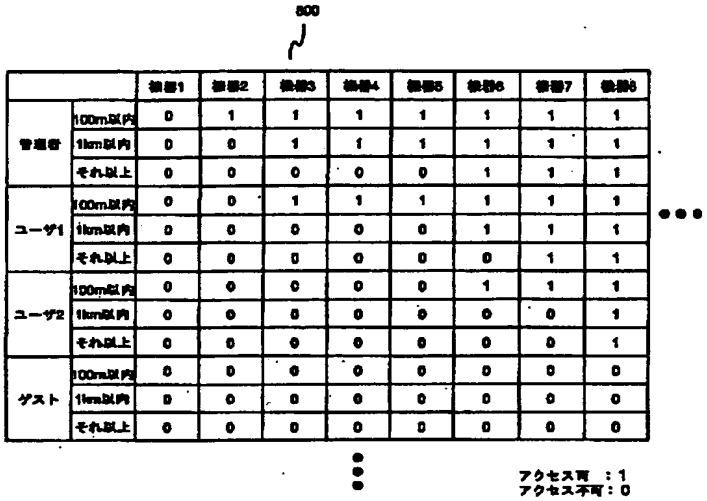
【図５】


600
601
602
メモリ部
ネットワークI/F部
処理部
603

【図６】

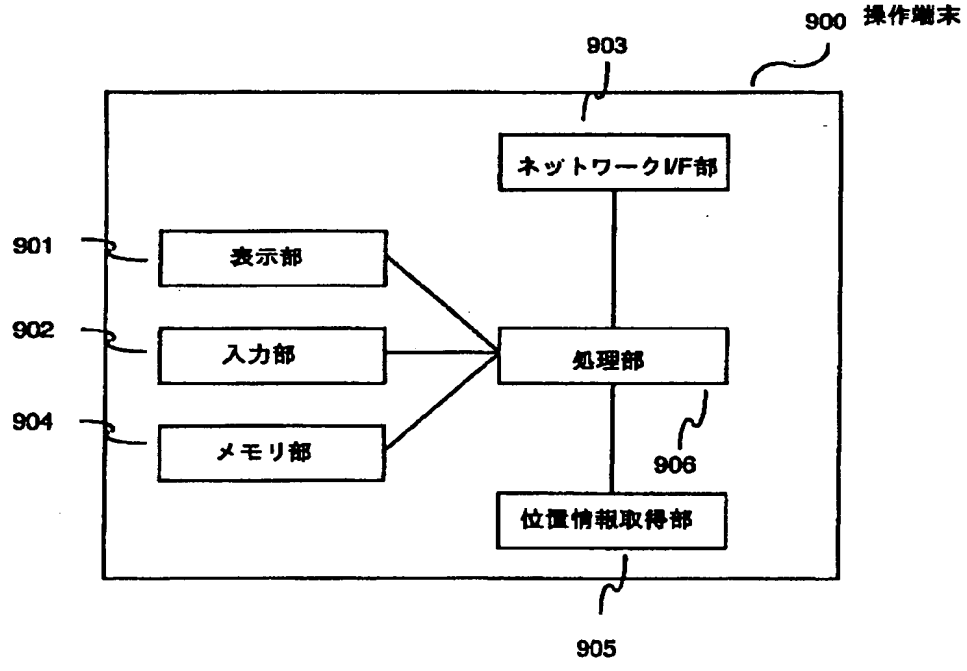

701
ログイン
702
コマンド入力待ち
703
制御コマンド入力
704
アクセス制御装置に確認
NO
制御不可であることを通知
706
YES
705
機器制御コマンド送信

【図７】

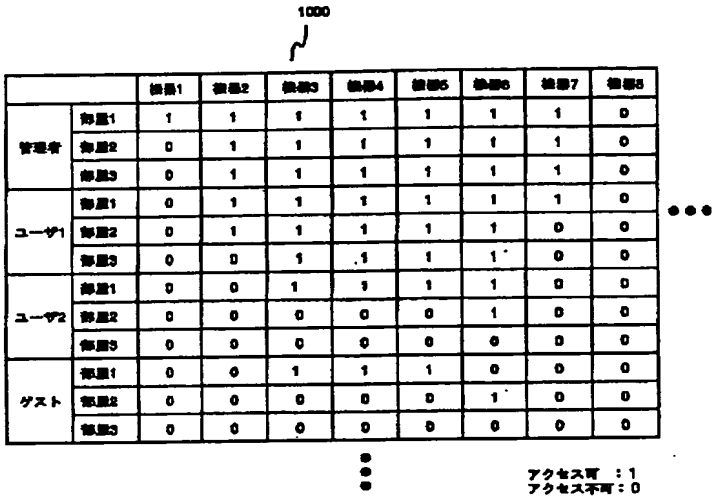


		機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
管理者	100m以内	0	1	1	1	1	1	1	1
	1km以内	0	0	1	1	1	1	1	1
	それ以上	0	0	0	0	0	1	1	1
ユーザ1	100m以内	0	0	1	1	1	1	1	1
	1km以内	0	0	0	0	0	1	1	1
	それ以上	0	0	0	0	0	0	1	1
ユーザ2	100m以内	0	0	0	0	0	1	1	1
	1km以内	0	0	0	0	0	0	0	1
	それ以上	0	0	0	0	0	0	0	1
ゲスト	100m以内	0	0	0	0	0	0	0	0
	1km以内	0	0	0	0	0	0	0	0
	それ以上	0	0	0	0	0	0	0	0

【図８】

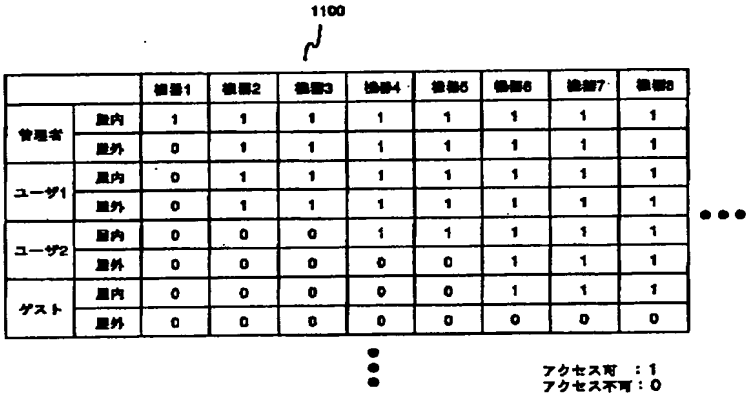


【図９】



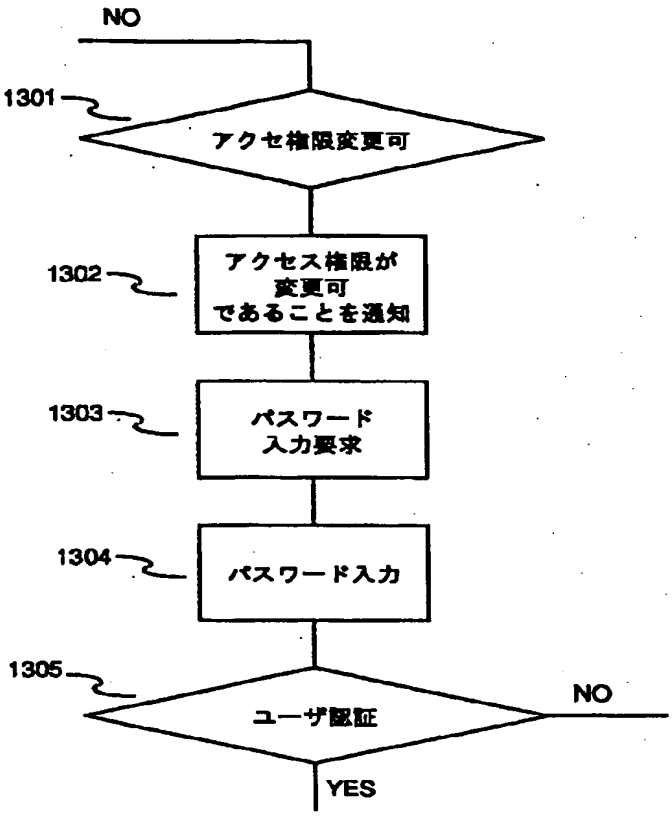
		機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
管理者	部屋1	1	1	1	1	1	1	1	0
	部屋2	0	1	1	1	1	1	1	0
	部屋3	0	1	1	1	1	1	1	0
ユーザ1	部屋1	0	1	1	1	1	1	1	0
	部屋2	0	1	1	1	1	1	0	0
	部屋3	0	0	1	1	1	1	0	0
ユーザ2	部屋1	0	0	1	1	1	1	0	0
	部屋2	0	0	0	0	0	1	0	0
	部屋3	0	0	0	0	0	0	0	0
ゲスト	部屋1	0	0	1	1	1	0	0	0
	部屋2	0	0	0	0	0	1	0	0
	部屋3	0	0	0	0	0	0	0	0

【図１０】



		機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
管理者	屋内	1	1	1	1	1	1	1	1
	屋外	0	1	1	1	1	1	1	1
ユーザ1	屋内	0	1	1	1	1	1	1	1
	屋外	0	1	1	1	1	1	1	1
ユーザ2	屋内	0	0	0	1	1	1	1	1
	屋外	0	0	0	0	0	1	1	1
ゲスト	屋内	0	0	0	0	0	1	1	1
	屋外	0	0	0	0	0	0	0	0

【図１２】


NO
1301
アクセス権限変更可
1302
アクセス権限が
変更可
であることを通知
1303
パスワード
入力要求
1304
パスワード入力
1305
ユーザ認証
NO
YES